OSJ OPEN SCIENCE JOURNAL

REVIEW

Enhancing Healthcare Information Sharing with Blockchain Technology

Tod Yates[1]*

[1]Franklin University, United States of America

*Corresponding author: Tod Yates: tod@tdyates.com

OPEN ACCESS

Citation: Yates T. (2020) Enhancing Healthcare Information Sharing with Blockchain Technology. Open Science Journal 5(2)

Received: 5th March 2020

Accepted: 24th April 2020

Published: 8th May 2020

Funding: The author[s] received no specific funding for this work

Competing Interests: The author has declared that no competing interests exists.

Abstract:

Blockchain, the foundation of many cryptocurrencies, also can be useful for many other industries such as healthcare. Blockchain can enforce immutability and non-repudiation for information stored on it. Although some say the technology is not yet mature enough, others are putting blockchain to the test with programs and pilots. Examining these efforts and dissecting the detail allows us to look at blockchain's qualities and pitfalls to allow data sharing efforts with medical records.

It is widely agreed that sharing medical data outside of the silos where it is captured or created will benefit the individual's care and outcomes. Regulation and personal humility often stand in the way of this sharing. Blockchain is offering new and novel ways to share data properly and securely with only the providers or researchers who are supposed to receive it. Blockchain is also allowing the patient to take control of their health data and in some cases, even profit from it.

Keywords: Blockchain, medical data, health data, data sharing, data silos

Introduction

In 2009 the United States Congress passed the American Recovery and Reinvestment Act, which included the Health Information Technology for Economic and Clinical Health Act (HITECH) [1]. HITECH spurred an enormous increase in the implementation of electronic health records (HER) under a guise known as "meaningful use" [1]. In 2008 non-federal acute care hospitals with EHRs were only 9% of the total, a number that leapt to 96% by 2015 [1].This created an unforeseen result that plagues U.S. healthcare today: data silos.

Despite ubiquitous broadband connectivity, the remaining paradigm for transferring digital medical images from the image generator to a patient's preferred primary care provider is by copying the image to a DVD, CD, or USB

stick and having the patient actually courier it themselves[2]. Zhou [3] also points to several factors that contribute to the data sharing problem in healthcare:

- Poor individual relationships
- Lack of trust
- Desire to retain professional power and status
- Lack of a conducive knowledge sharing culture
- Lack of absorptive capacity
- Lack of strong knowledge sharing leadership
- Inappropriate technological infrastructures
- Cultural affinity for autonomy
- Educational specializations and professions create obstacles to collaboration

Zhou goes on to note how crucial knowledge and knowledge sharing are to provide good, efficient patient care. Knowledge starts out as a single data point, then many data points about an individual, then by analysis of those data points we gain information or knowledge about many, which can then be applied to populations and becomes intelligence [4]. It is this intelligence that is restricted by regulation and personal humility.

For proper patient care, it is essential that data be shared among providers, pharmacies, insurance companies, and patient's families [5] Things get even more complicated when a patient moves from one hospital to another or even moves residence to another state [5]. Sending a medical record via the postal service is slow and emailing is not a secure channel for such sensitive information [5]. Health information exchanges try to act as an intermediary but are also part of the business of healthcare [1]. In order to get to a more patient-driven data sharing model, we need to consider a new technology: blockchain [1].

How blockchain can help

For obtaining long-term personal healthcare, data sharing is a must [6] Blockchain allows for transactions between entities without the need for trusted third parties [7]. This is achieved through distributed consensus, it is a way for untrusted parties in a transaction to trust in the facts of the transaction [7] Blockchain was introduced by the cryptocurrency Bitcoin in 2009 and it was the first solution to solve the double-spend problem: How to prevent someone from spending the same digital coin more than once [7]. This forced truth is known as immutability [7]. Blockchain is a distributed ledger, which means it is easy to audit and ensures the integrity of the data and prevents unauthorized changes [6]. O'Donoghue also asserts that a blockchain based electronic medical record system could shift the paradigm to a patient-driven model where patients control their data [6].

The existing medical data infrastructure depends in most cases on a trusted third party which cannot always be fully trusted [7]. Clearing houses and health information exchanges can have breaches [2]. Blockchain uses consensus among the members and does not rely on any third parties, which can be a solution to the problem [7].

Stakeholders and regulations

Data sharing that is secure and scalable is essential for patient care decisions and collaborative treatment [8]. This makes the patient and provider key stakeholders in the data sharing conversation. Also included are just about any healthcare professional, healthcare management organizations, government-managed health agencies, and patient relatives [3]. To broaden the scope, personnel in security and privacy and technical support staff, and offices of health information management can also be considered stakeholders [1].

Perhaps the most interested of stakeholders are researchers who will benefit from use of blockchain in a network of healthcare institutions and biobanks to gather patient data for research [5]. Funders of research and the ultimate beneficiaries, the public, are two more key stakeholders in the data sharing discussion [9].

As for regulations that affect stakeholders, they are myriad and complex. The most prominent is the Healthcare Information Portability and Accountability Act (HIPAA) [1]. The European Union recently adopted the General Data Protection Regulation (GDPR) which includes a right to be forgotten clause, which has a profound effect on the use of blockchain due to the immutability of data stored on it [1].

There exist justifiable reasons for protecting health data, but one can also make a strong ethical argument for using and sharing health data for the promotion of public health [10]. Public health agencies at the local and state level need timely local data in order to identify potential problems [10]. Schmit et al. go on to note that laws and regulations pose a barrier to data sharing due to the patchwork that is the United States data handling structure which protects data differently depending on the type of data, who owns it, why it was collected, and its intended use [10]. They also note that the law typically lacks specific authorizations to use data to improve public health [10].

Research questions

In order to investigate the utility of blockchain's ability to enhance data sharing and therefore data quality in healthcare, the following questions are proposed to guide our literature review:

1. Can blockchain technology improve data sharing in healthcare?
   What properties of blockchain can we take advantage of to cure the problems created by data silos and government regulation in order to share data about patient medical records that can lead to personal health plans based on intelligence?
2. Can blockchain enhance patient involvement in their health record?
   It was mentioned above that a patient-driven healthcare data structure is a desirable goal, but it is difficult with the current healthcare data infrastructure. What properties of blockchain can enable a patient to be more in control of their data? What risks might blockchain introduce or mitigate?
3. What is the current state of use of blockchain in healthcare?
   How are others using proof of concept or actual implementations in healthcare and what is the effect on data quality? What are some

possible future applications of blockchain? What are the weaknesses or risks introduced by blockchain that should be avoided?

Review of the literature

In the face of security challenges, the healthcare industry is grappling with pressures to share information, improve patient outcomes by discovering patterns, and discover new care models that work in a cost-effective and secure way for everyone [11]. Also, patients are more and more involved in managing their ailments by using Internet of Things [IoT] devices like mobile devices and wearable sensors [12]. Giordanengo goes on to note that patients are eager to participate in their care and that this type of involvement in data management has a positive effect on disease management [12]. Using blockchain, patients can share data with providers, payers, pharmaceuticals, themselves, and family [11].

This type of system allows the providers access to the most accurate and up to date medical data, enabling the right type of care at the right time [11]. New and emerging blockchain systems provide an ecosystem where patients have ownership of their health data and can decide with whom they want to share their data and how [11]. These more complete and transparent sets of patient data allow the medical system as a whole to press the definition of an accurate diagnosis, create high performing pharmaceuticals and effective care plans, plus providing a longitudinal record of a patient's care, all enabled by blockchain [11]. Shabani states that it just may be possible that blockchain-enabled solutions may actually change the culture of data sharing [13].

IoT devices and wearables generate huge amounts of health-related data [14] Zheng et al. go on to say that distributed ledger technologies like blockchain can improve health-related data sharing greatly. They also add that the benefit of sharing this data can aid stakeholders from patients and device users to companies and researchers and can contribute to the public health care system overall [14]. This data sharing can lead to predictive diagnostics, prevention of expensive tests, and fewer costly procedures [11]. There is movement toward this idea as over 150 blockchain projects as of 2019 had raised over $660 million [15]. Based on its merits, blockchain has been implemented in fields such as e-commerce, logistics, trading, and is rapidly growing in healthcare [16].

Blockchain projects today

Blockchain is making headway in some substantial projects in healthcare as demonstrated by the examples below.

Encrypgen – This offering puts the patient in charge of their genetic data by providing a platform that facilitates the searching, storing, buying and selling of an individual's genetic data. Individuals have the option to allow researchers to search for and purchase their data. Encrypgen is a private blockchain, meaning one must purchase a license to participate [13].

MedRec – Much like a health information exchange, MedRec allows for data exchange between jurisdictions. It is patient-vetted and enables the building of a holistic view of a person's health data, which can then be shared by the patient with selected viewers. MedRec handles authentication, accountability,

confidentiality, and data sharing, all important factors when dealing with sensitive data and all handled by the blockchain [13].

Nebula Genomics – Nebula Genomics takes advantage of the distributed nature of blockchain to avoid centralization as it connects data holders [individuals] and data buyers [researchers]. Individuals can share data while still maintaining ownership. Nebula Genomics removes any middlemen and empowers people with their own genomic data [13].

Blockchain issues

While blockchain can hold significant promise, there are also some challenges to overcome. Zheng et al. note that blockchain has problems such as cost, scalability, efficiency and data management flexibility [14]. They go on to note that transaction fees and centralization pose a risk, as does the possibility of a quantum computer attack [14]. Traditional blockchains, such as Bitcoin's, are inefficient and lack scalability with the Bitcoin network only able to process five transactions per second [14].

Some also point out that blockchain is unsuitable for storing medical records such as computed tomography scans that would only bloat the blockchain and made it unmanageable [12]. Giordanengo also notes that by revealing an individual's private key to a researcher or provider it essentially makes it public, so methods must allow for rescission of a key if permission to view data is reversed [12]. Finally, Giordanengo says that removing data from the blockchain, such as when a legal retention period expires, can subject an organization to risk because the immutability of blockchain holding on to that data is now a liability [12]. In May of 2018, Giordanengo concluded that blockchain is not yet mature enough to be used in a context of healthcare data [12].

Finally, researchers are faced with issues caused by governance bottlenecks and technical issues when it comes to data sharing [13]. Another issue researchers must deal with is that it can be difficult to segment out only the data of research interest and not the entire health record, which can place undue burden on them to protect data they do not want or care about [15].

Methodology

To understand how a blockchain functions, it is vital that one understands asymmetric encryption, also known as public key encryption [17]. A simple way to understand encryption is by example. There are many types of encryption, some stronger than others, so we will use one that is simple called MD2. Searching the internet using "online hashing algorithm" will produce many websites that allow one to hash a word, a phrase, or even an entire file using one of the many encryption schemes [17]. If we hash [encrypt] the phrase "Hello world" using MD2, we get the hash result of "195d5b5475ec3e6760f888511f20b84d". If we change the phrase to be "Hello World" [note the capital W], the hash result is "27454d000b8f9aaa97da6de8b394d986", quite a noticeable difference for such a small change. Both phrases will produce their same hashes no matter which website's MD2 algorithm is used and no matter how many times they are hashed.

Public key encryption uses a special type of hashing that produces a pair of hashes, or keys, known as a public key and an associated private key, and this is what makes blockchain secure [17]. If someone encodes a message with their public key, it can only be decrypted with the private key [17]. Likewise, if someone encodes a message with their private key, anyone with their public key can decode the message, which means that only the private key holder could have created the message, thus creating non-repudiation of the author [17]. In a blockchain scenario, a user's public key is how they are "known" to the blockchain and private keys stay just that, private [17]. When adding something to the blockchain, you sign it with your private key, meaning you and only you could have done it, and anyone can see it since your public key is known to the blockchain.

A blockchain is a network of computers called nodes [2].Those nodes are part of an untrusted peer to peer network that has a consensus mechanism to decide on how and when to add new blocks to the chain and by whom [2]. Trust is not necessary between peers because the consensus mechanism, or protocol, is made of identical computer code residing on each node that enforces immutability and non-repudiation [2]. Smart contracts are special code snippets that can also reside on the network nodes [18]. Smart contracts execute whenever certain conditions on the blockchain are met or when they are explicitly called by an external stimulus like a smartphone app [18]. Now that there is a level set on the technology of encryption and blockchain, exploring how others are using blockchain in healthcare will allow planning for a new implementation.

Research questions

It may help to revisit the research questions posed earlier at this point:

1. Can blockchain technology improve data sharing in healthcare?
2. Can blockchain enhance patient involvement in their health record?
3. What is the current state of use of blockchain in healthcare?

If we look back at two of the organizations mentioned earlier, MedRec and Nebula Genomics, we can examine in closer detail how they are using blockchain and gain insight into how it could be done. Electronic health records (EHRs) are very poor at making data retrieval easy across multiple institutions and/or geographies as life's events take the patient from place to place and provider to provider [18]. Ekblaw et al. have devised MedRec to address this issue. MedRec's blockchain does not actually store any protected health information (PHI), but instead stores three types of records: 1] A registrar record or patient identifier; 2] A patient/provider relationship record (PPR) that acknowledges a patient seeing a provider; and 3] A summary contract, or a record of whether the link between a registrar record [patient identifier] and a PPR allows data sharing [18]. The summary contract's state is set by the patient to not share, share just these particular things, or share everything [18]. The PHI stays secured in databases that can be securely accessed using smart contracts on the blockchain that check the three types of records noted above before allowing a data request to be fulfilled [18]. MedRec provides a longitudinal, immutable record of a patient's medical history and includes an auditable record of any PHI access and by whom [18].

Nebula Genomics has a different model for using one's genetic data. The company will sequence an individual's genomic data and provide it to them or permit them the opportunity to join the Nebula Genomic network [19]. Once in the network, the individual's identity is anonymized cryptographically [remember our earlier hashing exercise] and they can then choose to sell their genetic data to researchers and pharmaceutical companies [19]. Those buyers must remain transparent so the users know exactly how their data is being used [19]. All transactions are stored on the Nebula blockchain so that every consent to access data and by whom is immutably recorded [19].

Another idea for sharing medical images using blockchain leverages existing infrastructure made specifically for image sharing called DICOM (Digital Imaging and Communications in Medicine) [2]. In this system, unique identifiers (UIDs) are attached to images, which are then distributed through a clearinghouse by request from institutions or providers [2]. The clearinghouse presents a target for a breach, and Patel's blockchain proposal aims to remove the clearinghouse altogether [2].

In Patel's model, an image has its DICOM UID made available to requests through a URL [2]. The difference from the clearinghouse model is that permissions to access the image are granted by the patient to another hospital or provider [2]. In this model, each of three actors possesses their own public/private key pair: 1] The facility that created the image; 2] The patient; and 3] A new provider/specialist. When the image is created, the DICOM UID is signed by the facility that produced it using their private key, making them the owner of the image [2]. The patient then uses their own private key in conjunction with the facility's private key to sign an assertion that the image may be shared [2]. This means that the patient's public key can decode requests from a third party to ensure that the patient authorized access. The patient then sees a new provider, perhaps a specialist, and wants to share the image. The patient, along with the new provider, sign a request with their private keys that is sent to the URL where the image is stored [2]. Since both the patient and the new providers public keys can decrypt the request, the image owner [the facility that created it] can rest assured that the patient initiated the request and that the new provider is who they claim they are and only then the image can be shared. Every step of the way, events are recorded on a blockchain, providing an immutable record of what was created, when and by whom, the moment of consent to share, and a record of the request for and fulfillment of the image.

Conclusion

Sharing of medical and protected health information is a challenge. Government regulation and, in most cases, personal humility also factor in. The three examples provided (Medrec, Nebula Genomics, and Patel's DICOM imaging plan) show that blockchain technology can indeed provide a pathway to allow data sharing to take place safely and securely. Each of the three models appear on the surface to fit into current data protection laws in the U.S. and Europe. While each case focused on a narrow area of health care, the general idea for each of the three can be applied to other areas of health care as well.

As for patient involvement in their own health record, the blockchain public/private key pair technology has proven it can enable patient involvement if not outright stewardship. A longitudinal health record is key to predictive

diagnostics, avoidance of expensive tests and labwork, and averting costly and possibly risky procedures. Putting an individual in charge of their own health data can mean they can benefit both financially and healthwise from researcher's use of that data if they so choose. The data generated by a patient has for too long been stuck in individual provider or laboratory's electronic systems and now there is this technology that allows it to be shared at the patient's wishes.

Finally, the current state of use of blockchain in healthcare is novel and still maturing. Pilot programs and experiments continue and will prove which ideas flounder, and which succeed. If we think back to the early days of the internet, there was hysteria about what was possible, and money poured into dotcoms. The dotcom bubble burst eventually and was followed by a time of petulance, but the internet did not go away because of that. Blockchain seems to be following a similar path where some measure of hysteria may be subsiding, and the sullenness of burst dreams sinks in. Much as the internet has plateaued back to a highly productive platform, blockchain may also follow this path to resurgence. This is just one way to start a virtuous cycle of better population health with the patient in charge of their data using blockchain as its foundation.

Acknowledgements

Dr. Melody Rose of Franklin University for the intense rigor in the academic setting and for the encouragement to publish.

Dr. Dale Gooden of Franklin University for his excellent mentorship.

References:

1.Gordon, W. J., Catalini, C. [2018]. Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability. Comput Struct Biotechnol J. https://doi.org/10.1016/j.csbj.2018.06.003

2.Patel, V. [2019] A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. Health Informatics Journal. Vol. 25[4] 1398–1411. https://doi.org/10.1177/1460458218769699

3.Zhou, L. [2017] Patient-centered knowledge sharing in healthcare organizations-- Identifying the external barriers. Informatics for Health & Social Care. Vol. 42 Issue 4, p409-420. 12p. DOI: 10.1080/17538157.2016.1269106.

4.Hovenga, E., Grain, H. [Eds.][2013]. Health information governance in a digital environment. IOS Press. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/franklin-ebooks/detail.action?docID=1477322

5.Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., Wang, F. [2017] Secure and trustable electronic medical records sharing using blockchain. AMIA Annual Symposium Proceedings Archive. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5977675/.

6.O'Donoghue O; Vazirani AA; Brindley D; Meinert E. [2019] Design choices and trade-offs in health care blockchain implementations: Systematic review. Journal Of Medical Internet Research. DOI: 10.2196/12426

7.Holbl, M., Kompara, M., Kamisalic, A., Zlatolas, L.N. [2018] A systematic review of the use of blockchain in healthcare. Symmetry. Vol. 10 Issue 10, p470. 22p.

8.Zhang, P., White, J., Schmidt, D., Lenz, G., Rosenbloom, S. [2018] FHIRChain: Applying blockchain to securely and scalably share clinical data. Comput Struct Biotechnol J. https://doi.org/10.1016/j.csbj.2018.07.004

9.Kalkman, S., Mostert, M., Gerlinger, C., van Delden, J., and van Thiel, G. [2019] Responsible data sharing in international health research: a systematic review of principles and norms. BMC Med Ethics. DOI:10.1186/s12910-019-0359-9

10.Schmit, C., Kelly, K., Bernstein, J.[2019] Cross sector data sharing:Necessity, challenge, and hope. The Journal of Law, Medicine & Ethics. Vol 47[S2]: 83-86. DOI: 10.1177/1073110519857325

11.Quarre, F., Israel, A. [2017] Blockchain: Catalyst for new healthcare ecosystem: Healthcare needs a way to share data, uncover patterns leading to better patient outcomes, and discover models for care that work securely and cost-effectively. CIO Insight. Retrieved from https://search-ebscohost-com.links.franklin.edu/login.aspx?direct=trueanddb=cphandAN=124711106andsite=ehost-live

12.Giordanengo, A. [2019] Possible usages of smart contracts [blockchain] in healthcare and why no one is using them. International Medical Informatics Association. doi:10.3233/SHTI190292.

13.Shabani, M. [2019] Blockchain-based platforms for genomic data sharing: a de-centralized approach in response to the governance problems? Journal of the American Medical Informatics Association, Vol 26 [1]. https://doi.org/10.1093/jamia/ocy149

14.Zheng, X., Sun, S., Mukkamala, R., Vatrapu, R., Ordieres-Mere, J. [2019] Accelerating health data sharing: A solution based on the internet of things and distributed ledger technologies. Journal of Medical Internet Research. Vol 21 [6]. doi: 10.2196/13583.

15.Johnson, M., Jones, M., Shervey, M., Dudley, J., Zimmerman, N. [2019] Building a secure biomedical data sharing decentralized app [DApp]: Tutorial. Journal of Medical Internet Research. Vol. 21 [10]. Retrieved from https://web-b-ebscohost-com.links.franklin.edu/ehost/detail/detail?vid=0andsid=f23c699b-0da9-4852-adc1-dc79d301a686%40pdc-v-ssmgr03andbdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#AN=139431372anddb=lih

16.Rahmadika, S., Rhee, K. [2019] Toward privacy-preserving shared storage in untrusted blockchain p2p networks. Wireless Communications and Mobile Computing. https://doi.org/10.1155/2019/6219868

17.SSD [n.a.][2018] A deep dive on end-to-end encryption: how do public key encryption systems work? Surveillance Self Defense. Retrieved from https://ssd.eff.org/en/module/deep-dive-end-end-encryption-how-do-public-key-encryption-systems-work

18.Ekblaw, A., Azaria, A., Halamka, J. D., Lippmann, A. [2016] A case study for blockchain in healthcare:"MedRec" prototype for electronic health records and medical research data. [White paper].Retrievedfrom https://static1.squarespace.com/static/59aae5e9a803bb10bedeb03e/t/5a6fd2f7e2c48387dff12676/1517278000381/blockchain-medical-records-patient-data-medrec-eckblaw.pdf

19.B., Brennan. [2018] Nebula genomics: Blockchain-enabled genomic data sharing. Blockchain Healthcare Review. Retrieved from https://blockchainhealthcarereview.com/nebula-genomics-blockchain-enabled-genomic-data-sharing/